John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Class

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

BIANCA JOHNSTON on behalf of herself and all others similarly situated,

Plaintiff,

v.

ADOBE INC.,

Defendant.

Case No. 5:25-cv-03052

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Bianca Johnston ("Plaintiff") brings this class action complaint ("Complaint") on behalf of herself and a class of similarly situated California residents (the "Class Members") against Adobe Inc. ("Adobe" or "Defendant") for violations of the California Invasion of Privacy Act ("CIPA"), California Penal Code § 630, *et seq*., including § 631 with regard to the unauthorized collection, recording, and dissemination of Plaintiff's and Class Members' personal information, geolocation data, and communications, and § 638.51 in relation to Defendant's use of "pen register" and "trap and trace" tracking software on Plaintiff's and Class Members' mobile devices in violation of federal law. Plaintiff also brings claims for Adobe's violation of her and other Class Members' right to privacy and for unjust enrichment. The allegations contained herein, which are based on Plaintiff's knowledge of facts pertaining to herself and her own actions and counsel's investigations, and upon information and belief as to all other matters, are as follows:

NATURE OF THE ACTION

1. Adobe is a multi-national software development company known for a range of publication and content creation software, including Adobe Photoshop and Acrobat Reader, and for creating the Portable Document Format.

2. This case is not about those products.

3. Rather, this case is about Adobe's practice of embedding its Tracking Tools[1] on thousands of websites and mobile applications, thereby allowing it to track, intercept, and monetize massive amounts of sensitive data pertaining to specific individuals.

4. The information that Adobe collects includes medical information, financial information, precise geolocation data, demographic information, political affiliation, and more.

5. Every second of every minute of the day, ordinary citizens are being spied on by companies like Adobe who—although not registered as a data broker in the state of California—

[1]As used throughout this Complaint, the term "Tracking Tools" refers to the various technologies Adobe uses to intercept, collect, and monetize data belonging to Plaintiff and Class Members. These tools include Adobe Audience Manager, Adobedtm.com, Adobe Dynamic Tag Management, Adobe Typekit, adobedc.net, Adobe Experience Cloud, Adobe Dynamic, Adobe SDKs, and the numerous other software evidenced in paragraphs 57-94 of this Complaint.

nonetheless operates within a gray area collecting, sharing, and profiting from consumers' data without their knowledge or consent.

6. Consider the average person who starts their day by checking the weather, local news, and traffic conditions before starting their commute to work or school. Within a matter of 10 minutes, they've used three or four different mobile applications.

7. At lunch, they read the latest political headlines, search for over-the-counter medications to treat chronic symptoms they're experiencing, and log into their retirement account. On their drive home, they drop off clothing donations at a church or synagogue, stop at a pharmacy to pick up a monthly prescription, and get brake-checked by a bad driver on the way home. When they get home, they search their teen's whereabouts using a family safety app, place an online order, and search for "low-carb recipes" while making dinner.

8. Each step of the way, every single interaction is being tracked, intercepted, repackaged and monetized by Adobe without the person's knowledge or control as the result of its pervasive practice of embedded its Tracking Tools into thousands of websites and mobile applications.

9. What to all the world looks like an ordinary day in the lives of many Americans is indeed an opportunity for the collection and monetization of highly-sensitive data which includes information about a person's religious beliefs, place of worship, political beliefs, medical conditions, immigration status, financial well-being, income, and more.

10. This information is not just being captured for the sake of pure data collection.

11. Instead, it's being sold to the highest bidder for advertising new products and services. It's being used to raise car insurance premiums. It's being used to make inferences about a person's actual medical conditions based on their internet search history and thereby raise medical insurance premiums. It's even being used by federal agencies that have been caught

buying up troves of information that would otherwise be unavailable to them without first obtaining a search warrant.

12. The efforts of privacy-conscious individuals to avoid the improper collection and storage of personal information—particularly sensitive personal information—must be protected. As the Supreme Court recognized in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), location data is highly sensitive, not just because of what the data point alone says about an individual (*i.e.*, where they were at a particular time), but also because of the massive amount of personal information that can be extracted from location data (such as medical treatment, personal relationships, and private interests).

13. As Chief Justice John Roberts stated, "a cell phone—almost a 'feature of human anatomy'—tracks nearly exactly the movements of its owner. . . . A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales," and when a third-party has access to the information stored on one's cell phone, that entity "achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id*. at 2218 (internal citations omitted).

14. Adobe represents one of the largest offenders in this insidious world of hidden data collection and resale.

15. Adobe has developed and disseminated a software development kit that enables backdoor access to consumers' devices and opens a direct data collection pipeline to Adobe and its advertising platform monetization partners.

16. Consequently, Plaintiff brings this action for legal and equitable remedies to address and rectify the illegal conduct and actions described herein.

17. As a result of Adobe's conduct, Plaintiff and Class Members have suffered numerous injuries, including invasion of privacy, loss of benefit of the bargain, diminution of value

of their private information, statutory damages, and the continued and ongoing risk to their private information.

18. Plaintiff seeks to remedy these harms and bring causes of action for (1) violations of Cal. Penal Code § 631, *et seq*.; (2) violations of Cal. Civ. Code § 56, *et seq*.; (3) violations of Cal. Bus. & Prof. Code § 17200, *et seq*.; (4) violations of Cal. Const. Art. 1 § 1; (5) violation of the Electronic Communications Privacy Act 18 U.S.C. § 2510, *et seq*.; (6) intrusion upon seclusion; (7) publication of private facts; and (8) breach of confidence.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) (the Class Action Fairness Act) because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and a member of the Class is a citizen of a different state than Adobe Inc. This Court also has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under 18 U.S.C. § 2510, *et seq.* (the Electronic Communications Privacy Act).

20. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

21. This Court has personal jurisdiction over Defendant because its corporate headquarters is located in this District.

22. Venue is proper in this District because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District. Moreover, Defendant's principal place of business is in this District, and the conduct alleged in this Complaint occurred in this District.

DIVISIONAL ASSIGNMENT

23. Pursuant to L.R. 3-2(c), assignment to this division is proper because a substantial part of the conduct which gives rise to Plaintiff's claims occurred in this District. Adobe's conduct

as described below is directed at Internet users and people throughout the United States, including Santa Clara County, California.

THE PARTIES

24. Plaintiff Bianca Johnston is an adult citizen and resident of the State of California and is domiciled in Big Bear, California. Plaintiff Johnston was in California when she accessed websites and mobile applications that contain Adobe's Tracking Tools. Plaintiff Johnston does not have an Adobe account or any direct relationship with Adobe.

25. Adobe Inc., is a Delaware corporation with its principal place of business located in San Jose, California.

FACTUAL ALLEGATIONS

A. The California Invasion of Privacy Act

26. The California Constitutions recognizes the right to privacy inherent in all residents of the State. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety happiness, and privacy."

27. In 1972, through the Proposition 11 "Right to Privacy Initiative," the right to privacy was added to the California Constitution in order to codify this inalienable right and protect ordinary citizens from invasions of privacy at the hands of government actors and private entities alike.

28. "The right of privacy is the right to be left alone. It is a fundamental and compelling interest. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information." Ballot Pamp., Proposed Stats. and Amends. to Cal. Const.

with arguments to voters, Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27; *see also Hill v. Colorado*, 530 U.S. 703, 716 (2000) (the right to privacy includes right to be free in one's home from unwanted communication); *Hill v. National Collegiate Athletic Assn*., (1994) 7 Cal.4th 1, 81, (Mosk, J., dissenting).

29. Likewise, the California Legislature enacted the California Invasion of Privacy Act ("CIPA") to protect the privacy rights of California citizens. In doing so, the California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

30. CIPA prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from or received at any place within California.

31. To establish liability under CIPA, Plaintiff need only establish that Adobe does, or did, any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system; or
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state; or
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or

> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

32. Violations of CIPA are not limited to phone lines but also apply to "new technologies" such as computers, the Internet, and email.[2]

33. CIPA affords a private right of action to any person who has been subjected to a violation of the statute to seek injunctive relief and statutory damages of $5,000 per violation, regardless as to whether they suffered actual damages. Cal. Penal Code § 637.2(a)(1).

34. Moreover, CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

35. A "pen register" is a "device or process that records or decodes dialing, rerouting, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

36. By contrast, a "trap and trace device" is a "device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." *Id.*

37. A "pen register" is a "device or process" that records outgoing information, whereas a "trap and trace device" is a "device or process" that records incoming information.

38. Although CIPA was enacted before the creation of the Tracking Technologies discussed in this Complaint, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google*

[2] *See In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

Inc. 2013 WL 5423918, at *21 (N.D. Cal. Sep. 26, 2013); *see also, e.g., Shah v. Fandom, Inc*, --- F. Supp. 3d ---, 2024 WL 4539577, at *21 (N.D. Cal. Oct. 21, 2024) (finding trackers similar to those at issue here were "pen registers" and noting "California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted"); *Mirmalek v. Los Angeles Times Communications LLC*, 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024) (same); *Moody v. C2 Educ. Sys. Inc.*--- F. Supp. 3d ---, 2024 WL 3561367, at *3 (C.D. Cal. July 25, 2024) ("Plaintiff's allegations that the TikTok Software is embedded in the Website and collects information from visitors plausibly falls within the scope of §§ 638.50 and 638.51."); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) (referencing CIPA's "expansive language" when finding software was a "pen register"); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications."). This accords with the fact that, "when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc*., 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

39. Individuals may bring an action against the violator of any provision of CIPA, including § 638.51, for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

B. How Tracking Technologies Invisibly and Covertly Harvest Information

40. Businesses like Adobe collect information about citizens by using a broad range of online technologies to track, monitor, collect, and assemble internet-based interactions and communications.

41. "Identity Resolution" services, such as those offered by Adobe, use profiling to link data from different websites in order to build user profiles based on browsing history, mobile app usage, and other information.

42. In conjunction with this process, companies like Adobe rely on persistent identifiers—including IP addresses, universal resource locators, mobile advertising identifiers, and more—to track individuals across multiple websites.

43. As the name suggests, persistent identifiers are a set string of numbers and/or letters that are used to track a specific individual from website to website or app to app.

44. Adobe knowingly and intentionally developed its persistent identifiers in order to track individuals—including Plaintiff and member of the Class—across internet-connected services despite knowing that the creation and use of these identifiers defies ordinary consumers' expectation of privacy.

45. For example, the Adobe Experience Cloud ID (ECID) and similar tools were designed to track users that have taken privacy-preserving steps.

46. **Tracking Cookies.** Tracking Cookies are small text files that websites place on a user's web browser to collect data about their online activities. These files contain data that allows websites to track user behavior across different websites. Tracking cookies are a type of persistent identifier wherein the identifier itself is stored within the cookie, thereby enabling websites to recognize and differentiate individual users. When a user visits a website, it may set both first-party cookies and third-party cookies on the user's web browser. Importantly, users cannot merely "opt-out" of cookies as is often suggested by consent banners and ad blockers, and this is particularly true regarding first-party cookies.

47. Tracking cookies can collect, process, and share all kinds of sensitive data from users, including: search and browser history; language preferences; IP address; on-site behavior

like link or button clicks, pages visited, time spent on page; past purchases; search phrases; browser type; screen resolution; ads seen and interacted with; and more.

48. Although Plaintiff is presently unaware of the full scale of Adobe's tracking via cookies, its current tracking efforts include the demdex and everresttech.net cookies, and "[t]he demdex cookie contains a Unique User ID (UIID)."[3] Likewise, "Adobe Advertising (formerly Adobe Advertising Cloud) uses cookies to map ad engagement events to conversion events and, potentially, to use that information to optimize ad bids."[4][5]

49. **Tracking Pixels.** A pixel, which may also be referred to as a "tracking pixel," "web bug," "clear GIF," or "web beacon," is a type of invisible tracking tool embedded in a website or an email to track a user's activities.

50. **Mobile Advertising ID ("MAID").** A MAID is a unique identifier assigned to a consumer's mobile device to assist marketers with advertising and identifying specific individuals. The MAID, which is also referred to as a "device_id_value," is sent alongside timestamped latitude and longitude coordinates. Like other persistent identifiers, a MAID is used to connect consumer activity to a specific individual and their real-world identity. According to the FTC, "MAIDs and other persistent identifiers, by design, enable direct communication with individual consumers, are used to amass profiles of individuals over time and across different web and mobile services, and are the basis to make decisions and insights about individual consumers."[6]

---

[3] https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/audience-manager (last accessed March 13, 2025).

[4] https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/advertising (last accessed March 13, 2025).

[6] *See In the Matter of Gravy Analytics, Inc., a corporation, and Venntel, Inc., a corporation* (Compl. 212-3025), available online at https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf (last accessed Jan. 4, 2025).

51. **Software Development Kits.** Software development kits ("SDKs") are pre-code software bundles that mobile application ("app") developers often use to minimize development work (instead of writing the entire app code from scratch) and to create a predictable stream of income that grows as more people use the app.

52. App developers embed SDKs into their apps that the developer did not themselves create and, therefore, may not know the full extent and function of the code in the SDK. Some SDKs, unbeknownst to consumers, siphon consumers' location data directly to a data broker or advertising platform, which can even include the ability to track users' locations through public Bluetooth beacons, which enable fine-grained tracking indoors.

53. **Server-side Tracking.** Server-side tracking, some times referred to as "server-to-server tracking," functions as a work around so that, even if third-party tracking cookies become wholly obsolete or are otherwise blocked by the consumer, online marketers can still identify individual websites visitors and/or app users. As the name implies, the communications flow from the website owner or app developer's server to another server.

54. In the case of Adobe, it offers several "server-side" tools such as its Experience Platform Web SDK, Edge Network API, Adobe Launch Server Side (also known as Adobe Experience Platform Data Collection Event Forwarding). These tools enable real-time event forwarding to other vendors and services (outside Adobe's ecosystem), but they also allow real-time sharing of analytics data to other Adobe Experience Cloud Solutions.

55. Adobe intentionally developed these tools to circumvent privacy measures.

56. **IP Address.** One important piece of identifying information collected by third-party trackers is a website user's IP address. An IP address is a unique identifier for a device, which is written as four sets of numbers separated by periods (e.g., 123.145.167.189). The first two sets of numbers reflect what network the device is on; the second two sets of numbers identify the

specific device. The IP address enables a device to communicate with another device, such as a computer's web browser communicating with a website server. An IP address is a unique numerical code associated with a specific internet-connected device on a computer network. A unique IP address identifies each of the devices accessing a certain network at any given time.

57. Significantly, an IP address contains geographical location information from which the state, city and zip code of a specific device can be determined. Given the information that it can and does reveal, an IP address is considered personally identifiable information and is subject to HIPAA protection.[7]

58. While IP addresses are unique, they are not necessarily "public" in the sense that they are freely accessible. If an individual is not actively sending data packets out, the IP address remains private and is not broadcast to the wider internet.

59. Knowing a website user's IP address, and therefore the user's geographic location, provides a level of specificity previously unfound in marketing. An IP address allows advertisers to target customers by countries, cities, neighborhoods and postal code. Even more specifically, it allows advertisers to target specific households, businesses and even individuals with ads that are relevant to their interests.[8]

60. Indeed, IP targeting is one of the most successful marketing techniques that companies can employ to spread the word about a product or service because companies can use an IP address to identify individuals personally.[9]

---

[7] *See* 45 C.F.R. § 164.514(b)(2)(i)(O).

[8] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LinkedIn (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businessesherbert-williams-z7bhf/

[9] Trey Titone, *The future of IP address as an advertising identifier*, Ad Tech Explained (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/

61. By targeting specific households or businesses, a company can avoid wasting money on ads that are unlikely to be seen by their target audience and can reach their target audience with greater precision. Additionally, by analyzing data regarding which households or businesses are responding to their ads, IP address targeting can help businesses improve their overall marketing strategies and refine their marketing efforts.[10]

C. Adobe's Collection of User Data

62. Adobe acknowledges that it collects vast amounts of data from users who visit websites and apps that have installed Adobe's tracking tools.

63. In addition to tracking the contents of consumer communications, Adobe tracks and collects precise geolocation data through IP Address Lookup, Adobe Target, Adobe "Launch," Adobe's Places Service, Mobile SDKs, and Plug-ins.

64. For example, Adobe's own documentation explains that its "getGeoCoordinates" plug-in allows you to capture the latitude and longitude of visitors' devices. Adobe recommends using this plug-in if you want to capture geo-location data in Analytics variables."[11] This allows software developers to use consumers' data in various ways, such as to "[t]arget a user with an in-store experience when relevant." It also interacts with other collected data, enabling developers to "[s]egment an audience based on offline behavior by using audience profiles with location context."[12]

[10] Herbert Williams, The Benefits of IP Address Targeting for Local Businesses, LinkedIn (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businessesherbert-williams-z7bhf/

[11] https://experienceleague.adobe.com/en/docs/analytics/implementation/vars/plugins/getgeocoordinates .

[12] *Id.*

65. But Adobe doesn't just give businesses access to geolocation data collected via that business's app or website. Rather, as Adobe explains, the Places Service allows businesses to "[a]nalyze foot traffic of your own stores *versus your competitor stores*."[13] In order to provide comparative foot traffic data, Adobe must collect and share consumers' geolocation data with other businesses that utilize Adobe's services, even if the consumer whose data is being brokered never downloaded, used, or agreed to location-sharing with that other developer.

66. Adobe describes its "Places Service" as "a geo-location service that enables mobile apps with location awareness to understand the location context by using rich and easy-to-use SDK interfaces accompanied by a flexible database of points of interests (POIs)."[14]

i. How Adobe Collects Web Browsing Data

67. Adobe uses its Tracking Tools in conjunction with persistent identifiers to track consumers across the internet as they browse different websites.

68. A portion of its tracking practices are described in part in its "Adobe Advertising Cookies" webpage.[15]

69. For example, Adobe's "everest tech" cookies, which can be identified by their link to everesttech.net and include both the "everest_g_v2 cookies" as well as the "id_adcloud" cookies help achieve this.

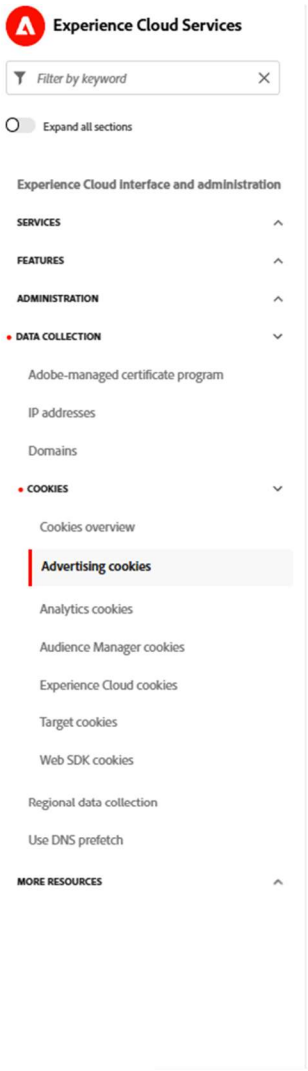
70. Both of these persistent cookies are used to track a specific user as they browse and communicate with the website in question, but they are also used to track an individual between different websites, amassing massive amounts of data for Adobe's advertising purposes.

---

[13] *Id.* (emphasis added).

[14] The Places Service Documentation. Available at https://experienceleague.adobe.com/docs/places/using/home.html (last accessed Sept. 8, 2024).

[15] https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/advertising



Adobe Advertising (formerly Adobe Advertising Cloud) uses cookies to map ad engagement events to conversion events and, potentially, to use that information to optimize ad bids.

NOTE

The beta Adobe Advertising Javascript tag that uses the Adobe Experience Cloud ID (ECID) Service creates first-party Experience Cloud `s_ecid` cookies, not Adobe Advertising cookies.

Cookie name	Expiration	Size	Location	Description
`_lcc`	15 minutes	52 bytes	`everesttech.net`	Stores IDs and timestamps of display clicks. Determines if a click event on a display ad applies to an Adobe Analytics hit.
`_tmae`	1 year	1 KB	`everesttech.net`	Stores encoded IDs and timestamps for ad engagements using DSP tracking. Includes user engagement with ads, such as ad last seen
`_tmid`	1 year	~20 bytes	`everesttech.net`	Stores the Adobe Advertising Demand Side Platform (DSP) ID. Corresponds to the visitor ID in the `everest_g_v2` cookie.
`adcloud`	1 year	50-150 bytes	First-party	The timestamps of the visitor's last visit to your website and the visitor's last search click. Also stores the `ef_id` that was created when the visitor clicked an ad. Ties the visitor ID with relevant audience segments and conversions. Helps optimize page load times by avoiding unnecessary requests to Adobe.
`ev_sync_*`		8 bytes	`everesttech.net`	The date when synchronization is performed in `yyymmdd` format. Syncs the Adobe Advertising visitor ID with the partner ad exchange. It is created for new visitors and sends a synchronization request when expired. Includes the cookies `ev_sync_ax`, `ev_sync_bk`, `ev_sync_dd`, `ev_sync_fs`, `ev_sync_ix`, `ev_sync_nx`, `ev_sync_ox`, `ev_sync_pm`, `ev_sync_rc`, `ev_sync_tm`, and `ev_sync_yh`.
`everest_g_v2`	1 year	~27 bytes	`everesttech.net`	Stores the browser and visitor ID. Created after a user initially clicks an ad. Used to map the current and subsequent clicsk with other events on your website.
`everest_session_v2`	Session	~16 bytes	`everesttech.net`	Stores the current session ID.
`id_adcloud`	91 days	16 bytes	First-party	Stores the visitor ID.

71. Adobe's Audience Manager is a tracking tool that works in conjunction with its demdex cookies, which are yet another persistent identifier used to track individuals across the internet.[16]

72. Adobe's Audience Manager tool is data management platform ("DMP"), which it uses to "[connect] known and pseudonymous data to create real-time, unified profiles ready for cross-channel activation."[17]

[16] https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/demdex-calls

[17] https://business.adobe.com/products/audience-manager/adobe-audience-manager.html

73. The Adobe Audience Manager is a pervasive tool that appears on 2,335 of the top 10,000 websites, including banking and retirement websites, healthcare websites, travel booking websites, and more.

74. Adobe's conduct is described further on the Adobe Audience Manager webpage, which explains that the Audience Manager relies on a few cookies to perform different functions, including, "things like assigning IDs, recording data calls . . . [and] [t]he demdex cookie helps Audience Manager perform basic functions, such as visitor identification, ID synchronization, segmentation, modeling, reporting, and so on."[18]

75. The "demdex" cookie has a lifespan of 180 days, so a person's unique ID follows them for 180 days *from the date of their last interaction with a partner website*, not 180 days total.[19]

76. This is just one of the many ways that Adobe uses its Tracking Tools to identify the same individual across multiple sites as they browse the internet.

77. As part of this process, Adobe engages in ID synchronization wherein it creates a unique visitor ID that links different online identifiers.

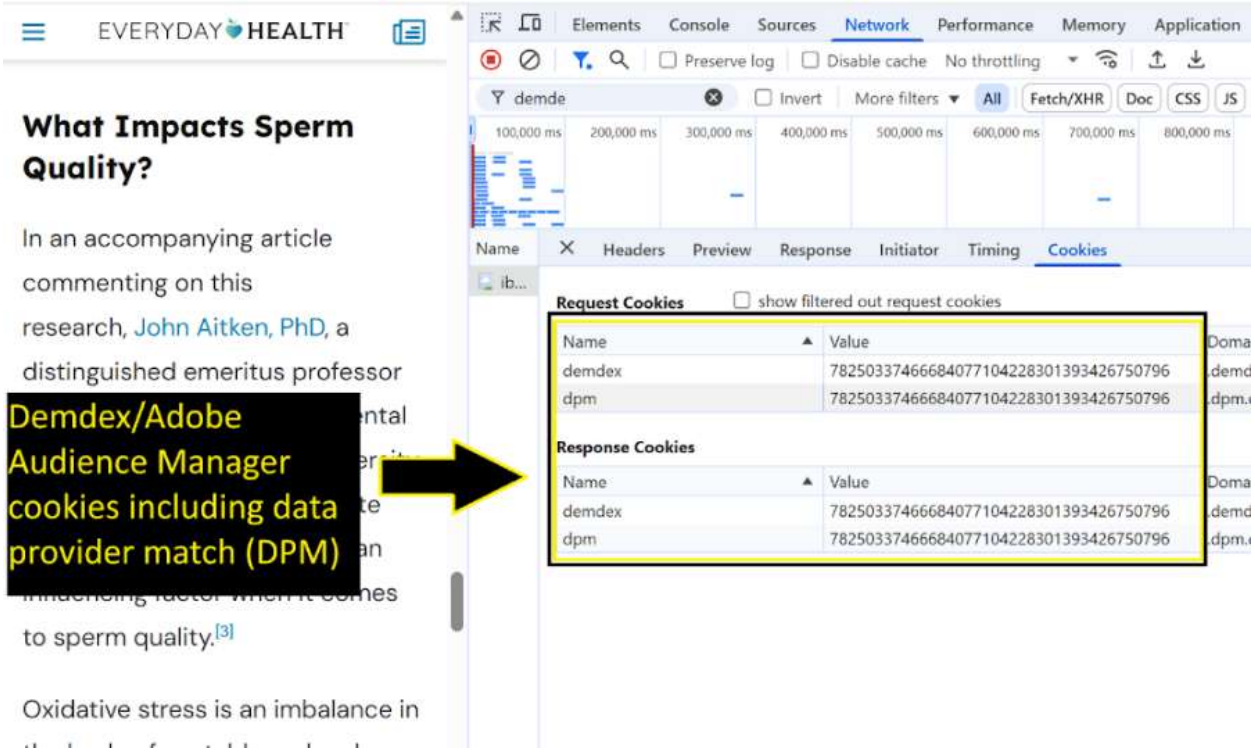
78. Adobe also segments users based on their interests and browsing activity for targeted advertisements based on inferred characteristics.

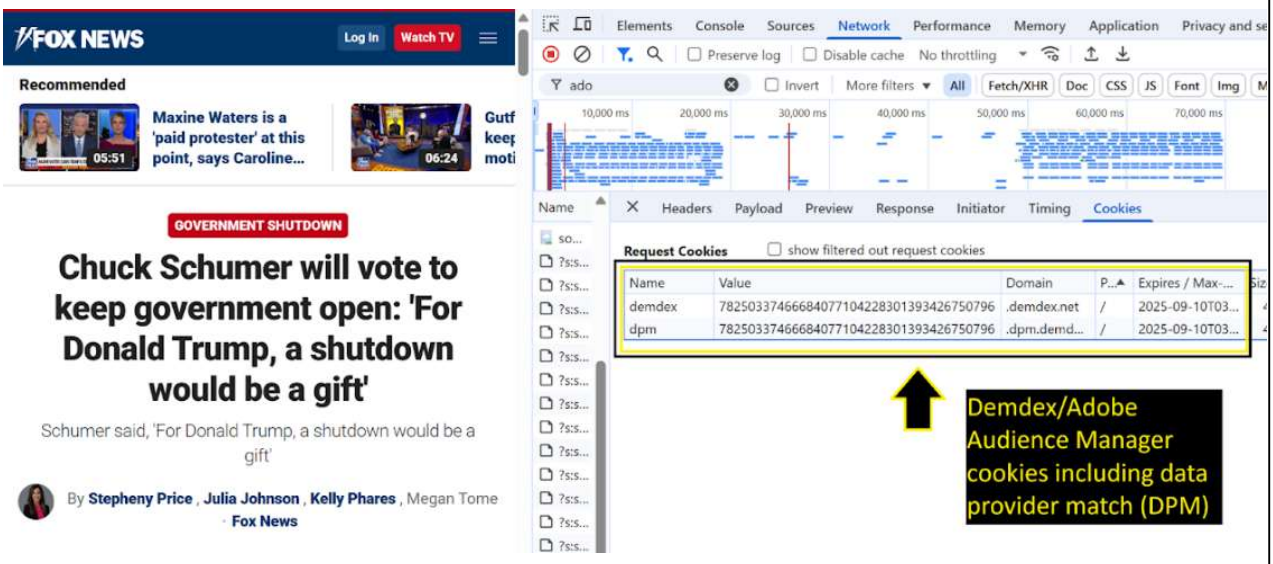
79. The images below demonstrate how Adobe follows website users across the internet as they browse different websites, amassing vast amounts of information in the process.

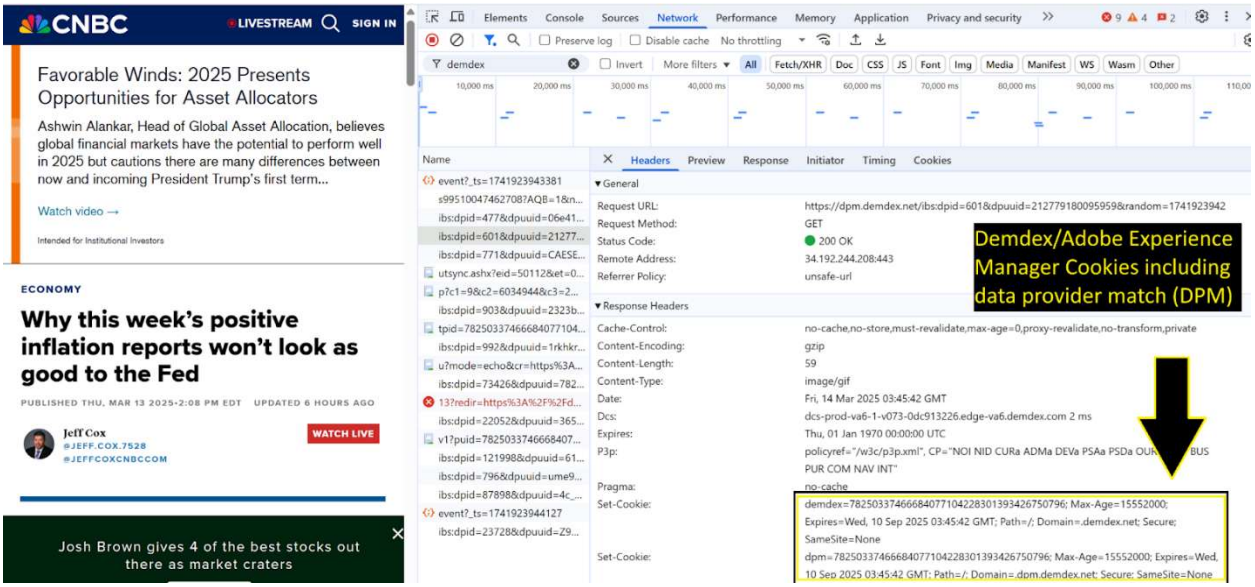
[18] https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/audience-manager

[19] This means that if a user visited several websites with the demdex cookie between 1/1/2024 and 1/1/2025 but does not visit another demdex-connected site until 06/29/2025, and proceeds to continue using demdex-connected sites until the end of 2025, Adobe will still be able to associate all of the 2024 browsing data with the browsing data from 2025, despite the ~730 day length of the entire time span, including a ~175 day period of consecutive non-use of demdex-connected sites.

80. For example, Adobe's invisible demdex tracker is embedded on Everyday Health, Fox News, and CNBC. This allows Adobe to tie a specific individual's online activity across those websites to a unique profile for Adobe's future use in advertising, marketing, and any other monetization activities.







81. In addition to the websites above, Adobe is also collecting information from thousands of website that gather sensitive health information, financial information, and more.

ii. How Adobe Collects App Usage Data

82. Adobe relies on its Tracking Tools to collect mobile application usage data in a similar fashion, and this process utilizes Adobe's mobile software development kits (SDKs).

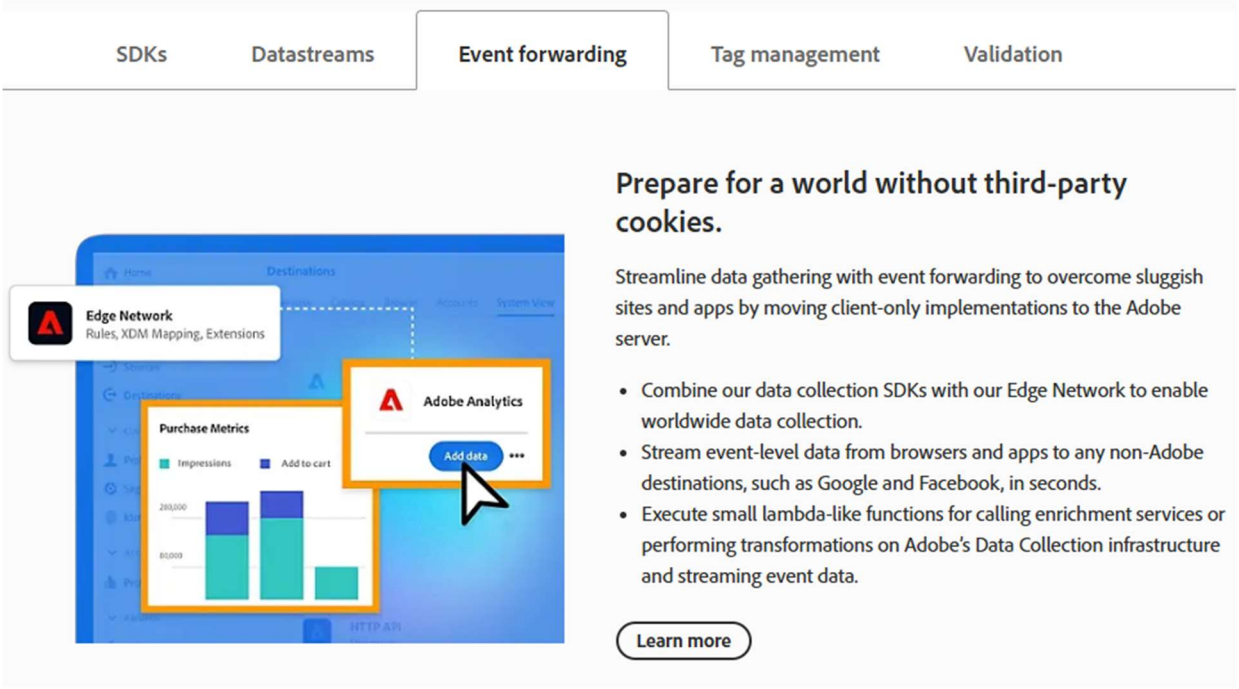
83. These SDKs are a collection of Adobe-created software tools that web and mobile app developers integrate into their applications to enable certain additional features.

84. In the case of Adobe's Experience Manager SDKs, developers gain the ability to instantly consolidate users' web activities with their corresponding mobile app activity through Adobe as well as the ability to utilize this data for targeted advertising, or to export the data to other services to be used for any number of purposes.

85. In turn, Adobe can also use this data for its own purposes and monetization, which it does via identity resolution services, real-time bidding, and other services that Adobe sells.

86. Adobe purposely designed its Tracking Tools to function and collect data without relying on third-party cookies, and this includes its data collection SDKs.

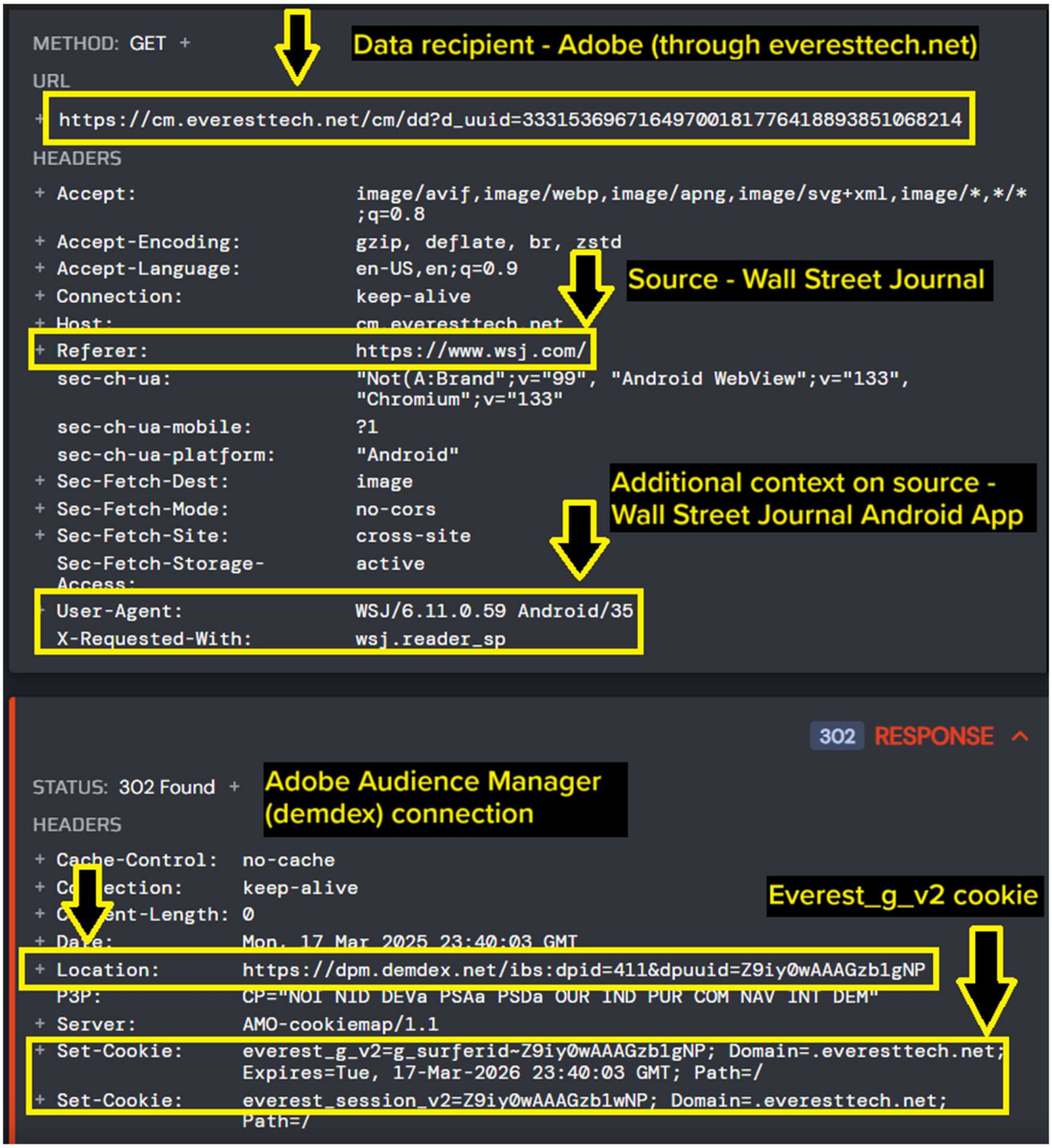
87. Adobe's own materials describe this, and Adobe promotes its tools to web developers stating "combine our data collection SDKs with our Edge Network to enable worldwide data collection."



88. Thus, Adobe collects data from mobile applications in much the same way it collects data from web browsers—*i.e.* by intercepting a person's interactions with a third-party application to build a comprehensive profile of that person's interests and activities to be used for targeted advertising.

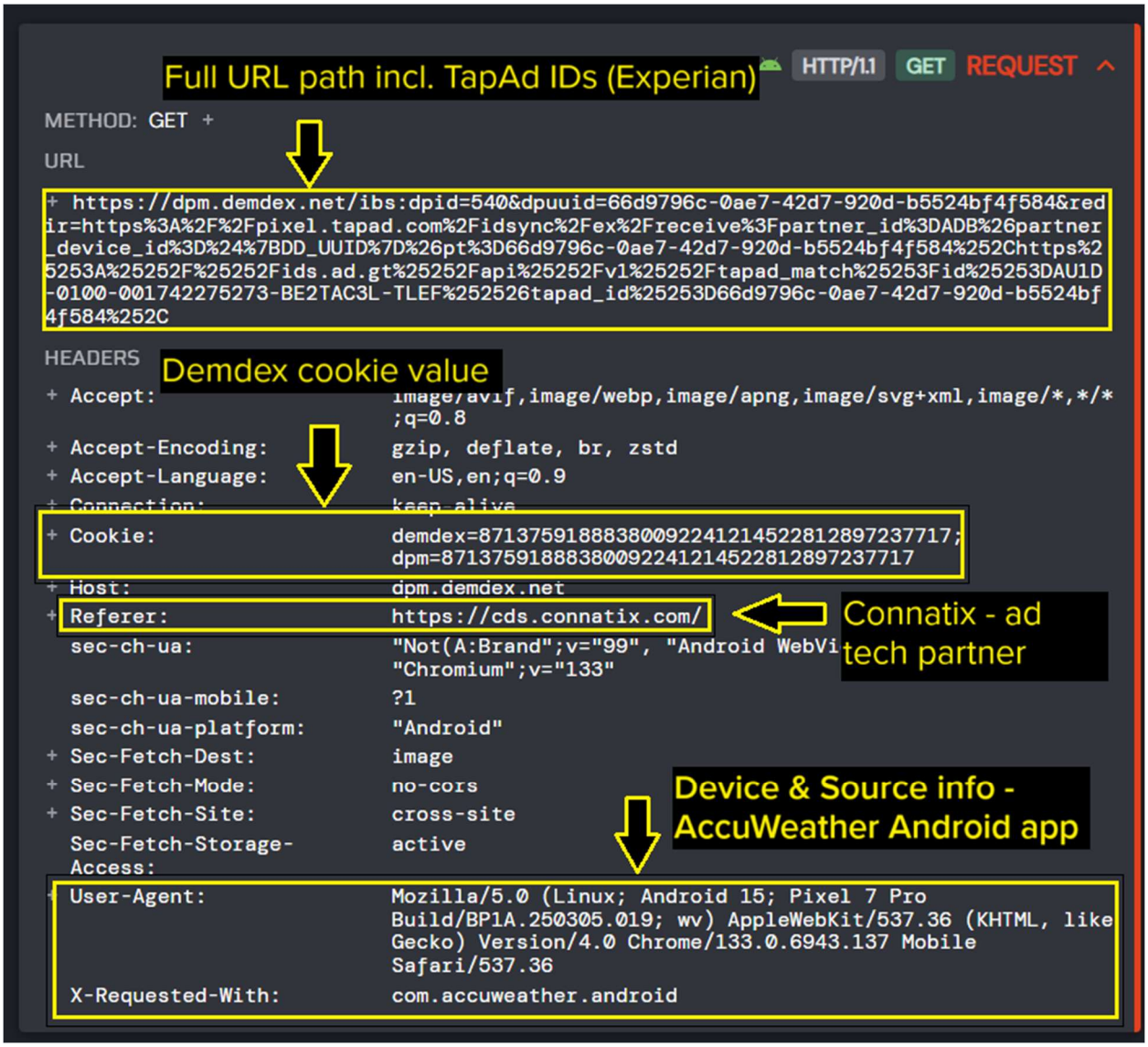
89. For example, the screenshots below show network traffic transmissions from two mobile applications—the CNN app and the Wall Street Journal app—which demonstrate that Adobe also uses its Tracking Tools in conjunction with its persistent identifiers ("demdex" and the "everest_g_v2" trackers) on mobile applications.


Content context info sent to Adobe - incl. article title
HTTP/1.1 POST REQUEST
2.1 kB Text REQUEST BODY
Additional context sent to Adobe - incl. source - CNN Mobile App
Demdex cookie/ID value



90. As depicted in the images above, the network traffic transmissions in the mobile app environment broadly mirror the network traffic transmissions in the web browsing environment - also containing cookies, the referrer URL indicating the publisher's site, and information about the device being used - all characteristics shared by the network traffic transmissions that Adobe receives from users' web browsing activities.

91. Certain network transmissions to Adobe also include partner ad tech companies' corresponding IDs, allowing Adobe to conduct identity resolution by associating third party IDs such as those from TapAd (Experian) and Connatix with Adobe's own "demdex" and "everest_g_v2" cookies through the identity resolution process ("ID synchronization").[20]



[20] https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/ids-in-aam

D. Adobe's Monetization of User Data

92. Adobe monetizes the wealth of information it collects via its Tracking Tools in variety of ways.

93. For example, Adobe engages in real-time bidding ("RTB") through its Adobe Advertising Cloud platform, which allows advertisers to access and bid on ad inventory in real-time, enabling more targeted and efficient ad placements across various digital platforms.

94. More specifically, Adobe operates what is known as a Demand-Side Platform ("DSP"). "The Adobe Advertising DSP centralizes purchasing and optimizes digital advertising inventory across various channels, formats, and publishers, from display and video to Connected TV (CTV). It unifies advertising tech with marketing tech, providing a more consistent user experience across every touchpoint."[21]

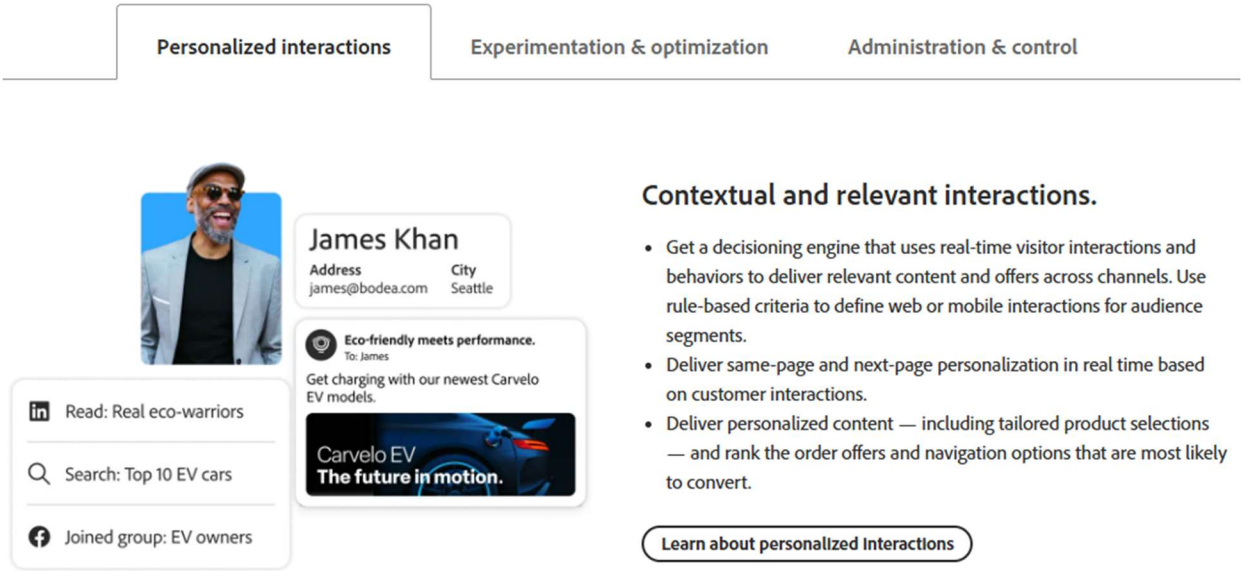
95. Adobe differentiates itself from other competitors in the RTB space by offering its customers an all-in-one platform with "Advanced Audience Targeting" that allows advertisers to target specific audiences based on demographics, interests, behavior, and location.

96. Adobe describes its Adobe Target tool as way to create personalized interactions: "With customizable AI algorithms and powerful integrations with Adobe Experience Platform, Target optimizes and personalizes the most important digital interactions to deliver greater revenue impact."[22]

[21] https://business.adobe.com/products/advertising/demand-side-platform.html (last accessed March 13, 2025).

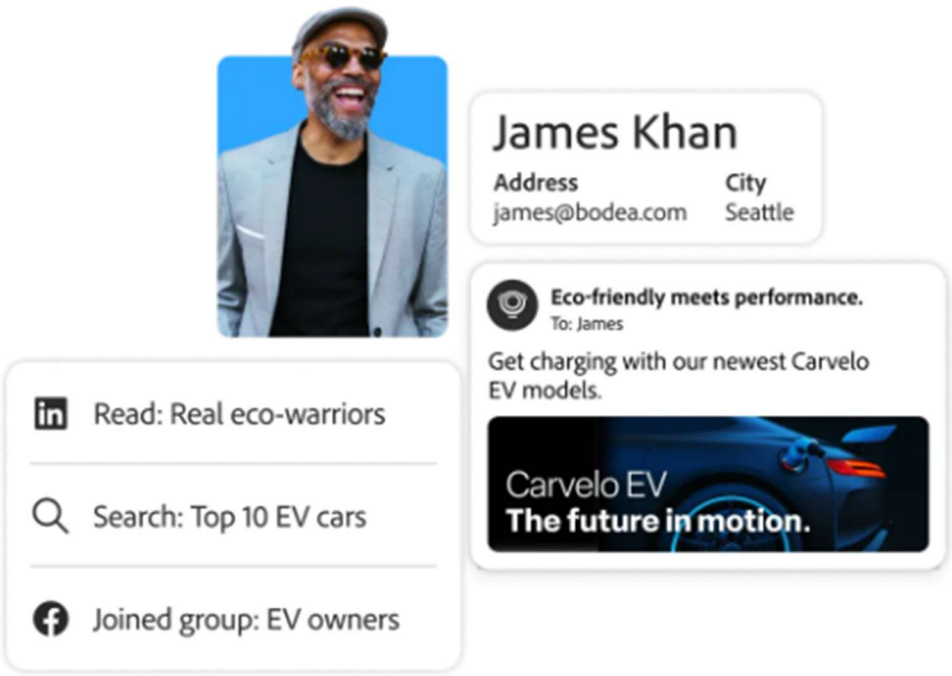
[22] https://business.adobe.com/products/target.html

97. The image below is an example of the type of information that Adobe gathers from across the internet and consumer devices, repackages, and sells to advertisers:[23]



98. As described by Adobe, the types of information it monetizes includes the consumer's name, city, email address, internet search history, the title of articles he's read on LinkedIn, and Facebook groups that the individual has joined in the past.

[23] Screenshot taken from Adobe's website, https://business.adobe.com/products/target.html on March 13, 2025.

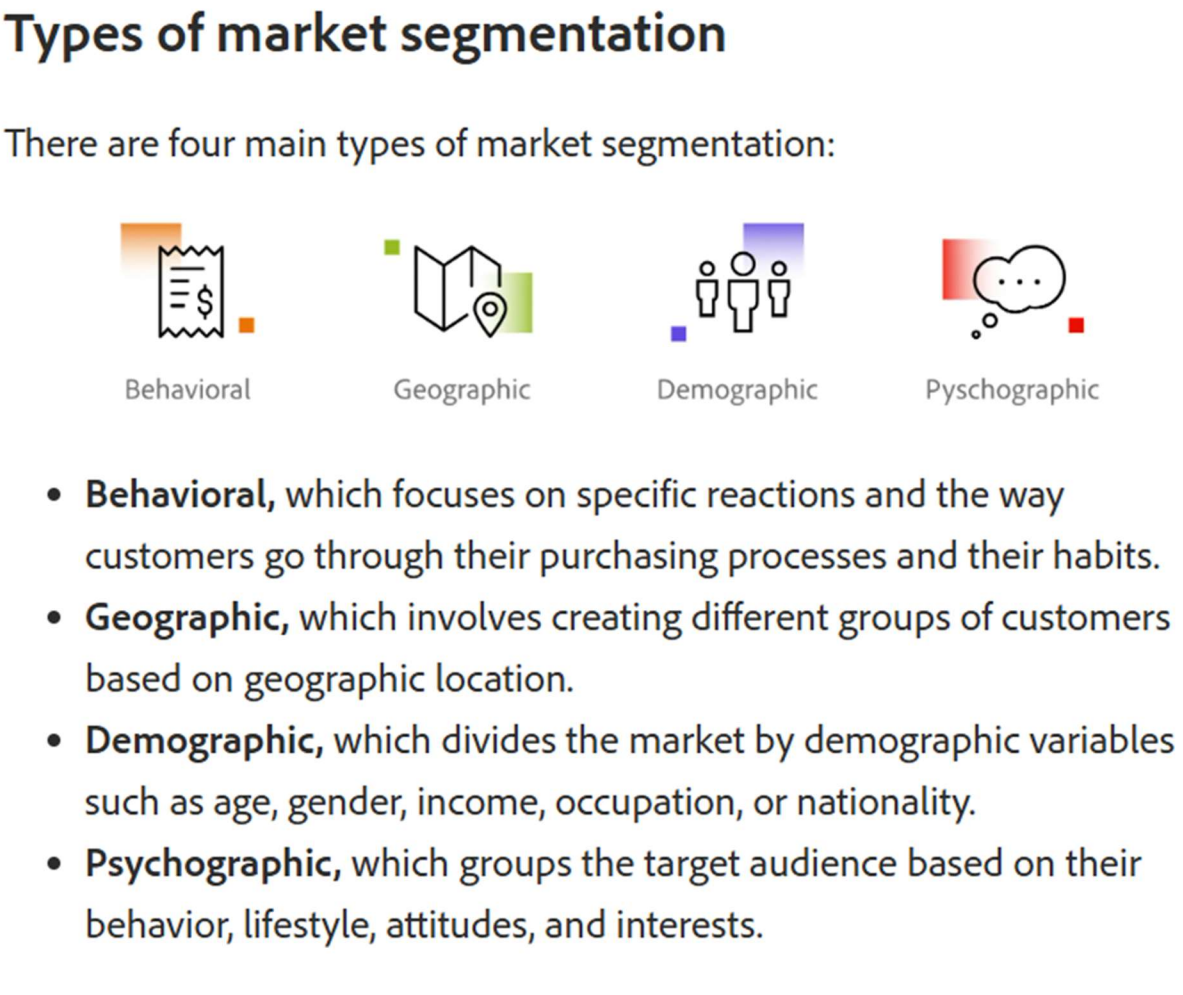


99. Adobe also offers a service called "Segment Match," which allows its customers to supply one another with additional data about a particular user based on that individual's device identifiers such as their IDFAs and GAIDs.

100. Adobe also utilizes market segmentation, which includes psychographic segmentation, demographic segmentation, geographic segmentation, and behavioral segmentation.

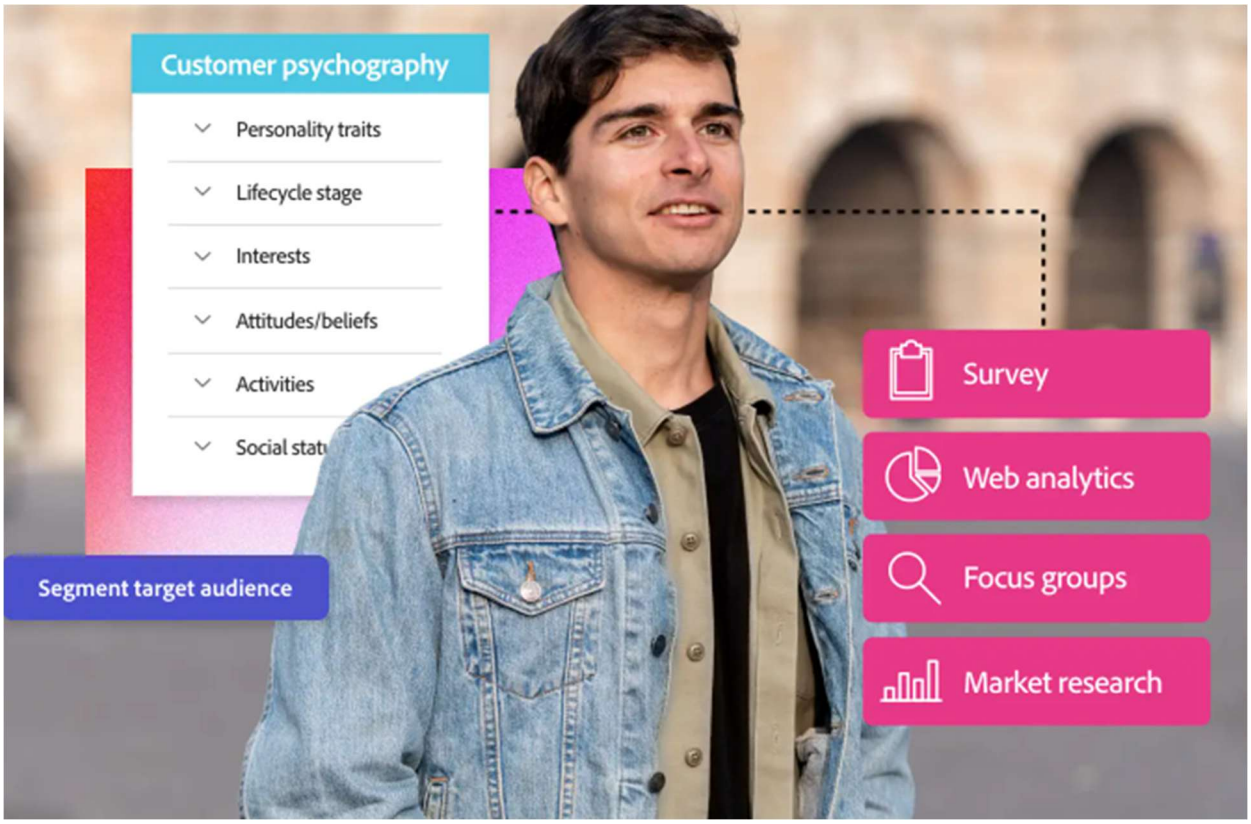
101. Adobe encourages its advertising partners to focus on gathering this type of information via their websites and mobile apps by using Adobe's Tracking Tools, and the infographic below was created to encourage and promote these intrusive practices.[24]

[24] https://business.adobe.com/blog/basics/get-a-quick-refresher-on-market-segmentation



102. For example, Adobe explains that "Psychographic data is a treasure trove for marketers who want to better understand the motivations behind why customers make the decisions they do. By analyzing a variety of different psychographic data points, you can build a more complete picture of who your customers are — and how you can solve their biggest pain points."[25]

[25] https://business.adobe.com/blog/basics/psychographics-examples#psychographics-vs-demographics



103. While harvesting and monetizing an individual's social status, hobbies, or interests is far from revolutionary, the more disturbing category of information gathering is "attitudes or beliefs," which includes sensitive information an individual may not want to share with their colleagues or friends, much less have it broadcast across Adobe's platforms.

104. Adobe also offers its users a "cookie-less" strategy with its Real-Time Customer Data Platforms ("Real-Time CDP"), which allows website owners and app developers to unify customer data from multiple sources in real-time.

E. Standing & Harm

105. Since America's founding, privacy has been a legally protected interest at the local, state, and federal levels. *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 1271-72 (9th Cir. 2019) (*quoting Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)) ("Privacy rights have long been regarded as 'providing a basis for a lawsuit in English or American courts.'"); and *Eichenberger*

v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017) ("Violations of the right to privacy have long been actionable at common law").

106. The invasion of privacy rights is a "concrete and particularized" injury sufficient to confer standing. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021) ("Various intangible harms can also be concrete [including] . . . disclosure of private information"); *In re Facebook Inc. Internet Tracking Litig*., 956 F.3d 589, 596 (9th Cir. 2020) (holding that Facebook's tracking of browsing histories that were sold to advertisers was an "invasion of [a] legally protected interest that is concrete and particularized").

107. Plaintiff alleges that she and Class Members were personally injured when Adobe impermissibly obtained their personal information, including data sufficient to enable Adobe to ascertain a user's location and track their website activity over time, and thus target that user with advertisements tailored to their location and/or browsing history.

108. It is black-letter law that such allegations are sufficient to confer Article III standing. *See, e.g., Mastel v. Miniclip SA*, 2021 WL 2983198, at *6 (E.D. Cal. July 15, 2021) (collection of "personal information without the plaintiff's consent involved a sufficiently 'concrete' injury"); *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F.Supp.3d 767, 784 (N.D. Cal. 2019)(dissemination to third parties of plaintiffs' personal information is "sufficient to confer [Article III] standing").

109. Separate from an invasion-of-privacy harm, Plaintiff also alleges economic harm sufficient for Article III standing by alleging that user data carries financial value, and by alleging that Adobe profited from the misappropriated data.

110. Courts regularly find such allegations sufficient to confer standing on plaintiffs alleging violations of their privacy rights under CIPA. See, e.g., *Shah v. Fandom, Inc.* __ F. Supp. 3d __, 2024 WL 4539577 (N.D. Cal. Oct. 21, 2024)(plaintiffs had standing based on allegations

that "the collection of their IP addresses through the Tracking Tools allows the third parties to obtain 'personally identifying, non-anonymized information,' and that the IP addresses reveal geographical location and other personal information sufficient for third parties to conduct targeted advertising"); *Mirmalek v. Los Angeles Times Comm'ns LLC*, 2024 WL 5102709, at *4 (N.D. Cal. Dec. 12, 2024) (same); *Moody v. C2 Educational Sys. Inc.,* 742 F. Supp. 3d 1072, 1078 (C.D. Cal. 2024) (plaintiff had standing based on allegations that defendant collected plaintiff's information, thereby constituting an invasion of privacy which is an "actionable injur[y]").

111. Adobe's interception, disclosure, and monetization of consumer data harmed Plaintiff and the Class. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data, and estimates for 2022 were as high as $434 per user, constituting over $200 billion industry wide.

112. The value of health data in particular is well-known. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data, observing that the market for this data is both lucrative and a significant risk to privacy.[26]

113. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig*., 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

[26] *See* https://time.com/4588104/medical-data-industry/ (last visited April 25, 2023).

114. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing historical information.

115. Personal information has private value beyond its use as a bare commodity.[27] The value of personal information is thus inherently related to the value of privacy, which is a question that has been researched in multiple fields including decision science, economics, information systems, management, health care, and marketing.[28] This research has approached the valuation of personal information from multiple perspectives:[29]

(a) The amount one would accept to relinquish their data;

(b) The amount one would spend to protect their data;

(c) The potential harm from data exposure; and

(d) The benefit a data holder could gain from acquiring data.

116. These approaches can be used to establish a set of data points for the reasonable estimation of the value of personal information and non-public medical information such as patient status.

117. In addition, numerous services exist that charge fees to monitor and remove personal information from data brokers and search databases. For example, Privacy Bee charges $197 per year.[30] Other similar services exist today, such as DeleteMe®, which removes

[27] Wagner, et. al (2018); Acquisti, Alessandro, Curtis Taylor, and Liad Wagman (2016); Li, Xiao-Bai, Xiaoping Liu, and Luvai Motiwalla (2021).

[28] Fehrenbach David, Carolina Herrando. "The effect of customer-perceived value when paying for a product with personal data: A real-life experimental study." *Journal of Business Research* 137 (2021): 222-232; Li, Xiao-Bai, Xiaoping Liu, and Luvai Motiwalla (2021); Alorwu, et al. (2024).

[29] Acquisti, Alessandro, Curtis Taylor, and Liad Wagman (2016).

[30] Privacy Bee - Pricing, privacybee.com, accessed September 26, 2024.

information from all major data broker websites for $129 per year,[31] deleteme™ which charges one-time fees ranging from $100 to $500 for search engine and data breach removals,[32] Incogni.com which charges $179 per year to remove information from major data broker websites and search databases,[33] and ReputationDefender, a service that charges $99 per year to remove personal information from various databases.[34] These provide a baseline market valuation of personal information

G. Adobe Obtains Consumer's Data without Consent

118. Adobe has a privacy policy that describes the information it collects through its vast range of data tracking tools, products, and services, but this policy is completely invisible to the users of the websites and mobile apps where Adobe's tracking tools are installed.

119. Additionally, Adobe's tracking tools are completely invisible when consumers use the websites and mobile apps where they are installed.

120. Users, including Plaintiff and Class Members, had no knowledge that while they were browsing websites or using mobile apps, that Adobe—a company completely unrelated to the website and/or app developers—was intercepting not only their browsing and app usage (including the contents of their communications), but also their location as they used their phones and other devices.

[31] Privacy Protection Plans - JoinDeleteMe, joindeleteme.com, accessed September 26, 2024.

[32] Deleteme - Services Pricing, deleteme.com, accessed September 26, 2024.

[33] Incogni – About Us, incogni.com, accessed September 26, 2024.

[34] ReputationDefender signup, me.reputationdefender.com, accessed September 26, 2024. ReputationDefender was previously known as Reputation.com and has been offering this service since at least 2012. Also see: https://www.nytimes.com/2012/12/09/business/company-envisions-vaults-for-personal-data.html

121. Users, including Plaintiff and Class Members, also had no knowledge that Adobe was aggregating the trove of data it collected to build highly detailed and sensitive profiles containing individual users' demographic information, location information, physical movements, and more.

122. Plaintiff and Class Members did not consent to Adobe's collection of their data, its repackaging, and/or monetization of that data.

123. By installing its Tracking Tools without Plaintiff's and Class Members' prior consent and without a court order, Adobe violated CIPA 638.51(a). In doing so, Adobe violated both Plaintiff's and Class Members' right to privacy and the control of their personal information. Adobe enriched itself by collecting Plaintiff's and Class Member's personal information and using it for marketing, advertising, identity resolution, analytics, and similar services that it offers and profits from.

Plaintiff Bianca Johnston

124. Plaintiff Bianca Johnston regularly visits websites and uses mobile apps that utilize and are embedded with Adobe's Tracking Tools, specifically including but not limited to: foxnews.com, walgreens.com, nypost.com, webmd.com, and weather.com.

125. Mrs. Johnston has used these apps and/or visited these websites consistently for several years, including during the last 3 months.

126. Mrs. Johnston regularly uses her mobile device to access the websites and apps listed above. On information and belief, through her use of these websites and apps, Adobe has tracked, collected, and monetized her geolocation, monitored and intercepted communications related to her personal characteristics, mode of living, purchase decisions, app selections, spending habits, medical information, and more.

127. By virtue of her use of the websites and apps listed above, Mrs. Johnston has unknowingly provided a wealth of data to Adobe, including her browsing history, search queries, IP address, geolocation, demographics, medical conditions (such as the sensitive private health information she communicated during her pregnancy), and more.

128. On information and belief, the data collected by Adobe has enabled it to build a profile of Mrs. Johnston that is so detailed that it is essentially de-anonymized.

129. Additionally, Adobe has provided its partners with identity resolution services and further monetized Mrs. Johnston's information by selling it during Adobe's real-time-bidding process.

130. Mrs. Johnston values her privacy, and she has never consented to Adobe's collection, monetization, and distribution of her personal data. Indeed, she was unaware that Adobe engaged in the course of conduct described throughout this complaint, and she never consented to Adobe's conduct.

131. Additionally, she did not provide her prior consent to Adobe's installation of its Tracking Tools on her browser or mobile device, its wiretapping of her communications, de-anonymization of her personal data, collection and further disclosure of her personal data, including information about her pregnancy, to advertising technology companies, data brokers, or any person or entity doing business with Adobe. Nor did Adobe obtain a court order to do the same.

132. Mrs. Johnston has, therefore, had her privacy invaded by Adobe's violations of CIPA §§ 631(a) and 638.51(a), and Adobe has been unjustly enriched by the disclosure and monetization of the improperly collected data concerning Mrs. Johnston.

TOLLING

133. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that her private information, data, and communications were intercepted, recorded, and monetized by Adobe.

CLASS ACTION ALLEGATIONS

134. **Class Definition:** Plaintiff brings this action on behalf of herself and other similarly situated individuals defined as follows:

> **Nationwide Class:** United States citizens who, during the class period, utilized websites that had Adobe's Tracking Tools embedded on their websites.
>
> **California Class:** All California residents who, during the Class Period, utilized websites that had Adobe's Tracking Tools embedded on their websites.

135. Plaintiff reserves the right to modify the class definitions or add sub-classes as needed prior to filing a motion for class certification.

136. The "Class Period" is the period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgment or preliminary approval of a settlement.

137. Excluded from the Class are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

138. Numerosity/Ascertainability. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff currently. However, it is estimated that there are thousands of individuals in the Class. The identity of such membership is readily ascertainable from Defendant's records and non-party records.

139. Typicality. Plaintiff's claims are typical of the claims of the Class because Plaintiff utilized websites that had Adobe's Tracking Tools embedded in them and had their personal identifiable information disclosed to third parties without their express written authorization or

knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

140. Adequacy. Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiff's interests are coincident with, and not antagonistic to, those of the Class Members. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the Class Members.

141. Common Questions of Law and Fact Predominate/Well Defined Community of Interest. Questions of law and fact common to the Class Members predominate over questions that may affect only individual Class Members because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Class:

(a) Whether Adobe intentionally tapped the lines of internet communications when it was not a party to those communications;

(b) Whether Adobe intentionally designed its Tracking Tools to surreptitiously track, intercept, and monetize consumers' data without first obtaining those consumers' consent;

(c) Whether Adobe installed and utilized a pen register and/or trap and trace device on consumers' mobile devices;

(d) Whether Adobe violated Plaintiff's and Class Members' privacy rights via its Tracking Tools and the conduct alleged herein;

(e) Whether Plaintiff and Class Members are entitled to damages under CIPA, the ECPA, or any other relevant statute(s);

(f) Whether Adobe's actions violated Plaintiff's and Class Members' privacy rights as provided by the California Constitution;

142. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit many similarly situated persons to

prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff is unaware of any special difficulty encountering in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 631, *et seq.*
(On Behalf of Plaintiff and the California Class)

143. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed Class.

144. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose.

> The Legislature thereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

145. California Penal Code § 631(a) provides, in pertinent part (emphasis added):

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or **who aids,**

> **agrees with, employs, or conspires** with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

146. Under CIPA, Adobe must show it had the consent of all parties to a communication, and that such consent was procured prior to the interception occurring.

147. Speaker of the California Assembly, Jesse Unruh, who introduced CIPA, urged that the law "represents an important advance in California law protecting the inherent rights of our citizens to privacy in their personal affairs. It is far stronger than the laws of many states in this field, and much tougher than the proposed federal eavesdropping legislation."[35] He further emphasized that the law would act as "a powerful deterrent to those who wiretap illegally for profit."[36]

148. Defendant's Tracking Tools are each a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

149. Adobe is a "separate legal entity that offer[s] [a] 'software-as-a-service's and not merely [] passive device[s]." *Saleh v. Nike, Inc*., 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, Adobe uses the wiretapped information for a purpose other than simply recording the communications and providing the communications to website operators—namely, its identity resolution services, real-time bidding platform, and other similar services that rely on its data collection capabilities in order to function. Accordingly, Defendants were each third parties to any communication between Plaintiff, on the one hand, and any of the websites and or apps at issue, on the other. *Id*. at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

150. Adobe's Tracking Tools are electronic listening devices that Adobe installed on Plaintiff's and Class Members' web browsers and devices that, without their knowledge and consent, read, attempted to read, and learned the contents of the electronic communications of

[35] July 31, 1967, Letter from Rep. Jesse M. Unruh to then California governor Ronald Reagan urging him to sign CIPA into law.

[36] *Id.*

Plaintiff, on the one hand, and the websites and mobile apps at issue, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

151. Adobe facilitated the interception and collection of Plaintiff's and Class Members' Private Information by embedding their tracking tools on various websites.

152. At all relevant times, Adobe uses those intercepted communications, including but not limited to building comprehensive user profiles that are further disclosure or sale in real time bidding to prospective advertisers.

153. Adobe's Tracking Tools constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, they fall under the broad catch-all category of "any other manner."

154. Plaintiff and Class Members did not provide their prior consent to Adobe's intentional interception, reading, learning, recording, collection, and usage of Plaintiff's and Class Members' electronic communications.

155. The wiretapping of Plaintiff and Class Members occurred in California, where Plaintiff and other Class Members accessed the websites, where Adobe's Tracking Tools were loaded on Plaintiff's and Class Members' browsers, and where Adobe routed Plaintiff's and Class Members' electronic communications to Adobe's servers.

156. As a result of the above violations, and pursuant to CIPA Section 637.2, Adobe is liable to Plaintiff and Class Members for treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the Plaintiffs have suffered, or be threatened with, actual damages."

157. Under the statute, Adobe is also liable for reasonable attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

SECOND CAUSE OF ACTION
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 638.51(a)

158. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

159. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

160. A "pen register" is a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of the communication." Cal. Penal Code § 638.50(b).

161. The Tracking Tools are "pen registers" because they are device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information" from Plaintiff and Class Members' electronic communications. *Id.*

162. At all relevant times, Adobe installed their Tracking Tools—which are pen registers—on Plaintiff's Class Members' browsers, which enabled Adobe to collect Plaintiff's and Class Members' IP addresses, geolocation, device information, and other persistent identifiers from the websites they visited. Defendants then used their Tracking Tools to build comprehensive user profiles, which were used to unjustly enrich Adobe and its clients by linking and enhancing Plaintiff's and Class Members' data when it is provided to advertisers through the real-time bidding process.

163. Plaintiff and Class Members did not provide their consent to Adobe's installation or use of the Tracking Tools.

164. Adobe did not obtain a court order to install or use any of their Tracking Tools.

165. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Adobe's violations of CIPA § 638.51(a), and each seek statutory damages of $5,000 for each of Adobe's violations of CIPA § 638.51(a).

THIRD CAUSE OF ACTION
Invasion of Privacy Under California's Constitution
(On Behalf of Plaintiff and the Class)

166. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

167. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted by California voters in 1972.

168. The addition of the phrase "and privacy" occurred after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Proposition 11 was intended to curb businesses' control over the unauthorized collection and use of peoples' personal information, as the ballot argument stated:

> The right of privacy is the right to be left alone. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.[37]

169. This amended constitutional provision addresses the concern over accelerating encroachment on personal freedom and security caused by increasing surveillance and data collection activity in contemporary society. Its proponents meant to afford individuals more measures of protection against this most modern threat to personal privacy:

> Computerization of records makes it possible to create 'cradle-to-grave' profiles of every American. At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian.[38]

In recognizing these privacy rights, the California Constitution provides insight into and serves to define the nature of the reasonable expectation of privacy of an objectively reasonable

[37] Ballot Pamp., Proposed Stats. & Amends. To Cal. Const. With Arguments to Voters. Gen. Election *26 (Nov. 7, 1972).
[38] *Id.*

California resident. In contravention to the California Constitution and the reasonable expectations of privacy of California residents, Adobe "stockpil[es] unnecessary information about [Class members] and [] misus[es]information gathered for one purpose in order to serve other purposes," creating "cradle-to-grave" profiles of Class members.

170. Plaintiff and Class Members maintain a reasonable expectation of privacy in the conduct of their lives, including their internet browsing activities and in their electronic communications and exchange of personal information. The reality of modern life increasingly requires that much of our daily activities are conducted online—Plaintiff and Class Members have no practical choice or ability but to conduct their daily lives substantially in the digital world, connected to the Internet. The necessary engagement with the digital world makes Plaintiff's and Class Members' private lives susceptible to unlawful observation and recording, capable of yielding a comprehensive and intrusive chronicle of Plaintiff's and Class Members' lives. If Plaintiff and Class Members cannot have a reasonable expectation of privacy in the conduct of their lives online and the digital transmission of their personal information, they can have no reasonable expectation of privacy for virtually any facet of their lives.

171. Adobe, in violation of Plaintiff's and Class Members' reasonable expectation of privacy, intercepts, collects, tracks, and compiles their internet activity and communications, and monetizes that data through third parties as well.

172. The nature and volume of the data collected is such that Adobe's practice of compiling comprehensive identity profiles violates Plaintiff's and Class Members' reasonable expectation of privacy. Technological advances, such as Adobe's use of Tracking Tools to compile internet activity and electronic communications, provide Adobe with the means to assemble a comprehensive chronicle of Plaintiff's and Class Members' lives heretofore unseen. Adobe collects and compiles personal information such as Plaintiff's and Class Members' names, postal addresses, email addresses, phone numbers, cookies, mobile device IDs, and web browsing information. Such information is "personal information" under California law, which defines personal information as including "[i]nternet or other electronic network activity information,"

such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

173. Adobe also collects and analyzes Plaintiff's and Class Members' real-world offline activity and compiles computerized records of those activities. Plaintiff and Class Members do not and cannot know which specific real-world offline activities Adobe may or may not be collecting and analyzing and adding to the digital dossiers it compiles on them.

174. Adobe's conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

a. Adobe engages in dragnet-style collection and interception of Plaintiff's and Class Members' Internet activity, including their communications with websites, without their consent.

b. Adobe also collects details about Plaintiff's and Class Members' *offline* activities. By its very nature, Plaintiff and Class Members cannot be aware of this.

c. Adobe creates comprehensive identity profiles based on this online and offline data, which constitute precisely the sort of "cradle-to-grave profiles" the right to privacy under the California Constitution was created to constrain.

175. Adobe's amassing of electronic information reflecting highly detailed aspects of Plaintiff's and Class Members' lives into dossiers, both directly and through providing access to its "Segment Match", for future or present use, is in and of itself a violation of Plaintiff's and Class Members' right to privacy in light of the serious risk these dossiers pose to their autonomy. Additionally, these dossiers are and can be used to further invade Plaintiff's privacy by, inter alia, allowing third parties to learn intimate details of Plaintiff's and Class Members' lives, and target them for advertising, political, and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them. Additionally, as described above, the social harms posed by Adobe's conduct impair not only individual autonomy, but the collective autonomy of Class Members, and autonomy is essential to the proper functioning of democratic republics.

176. Adobe's practices as alleged herein violate Plaintiff's and Class Members' reasonable expectation of privacy, are highly offensive to a reasonable person, and constitute an egregious breach of the social norms.

177. Adobe's violation of various state and federal statutes, and its actions to enable others to violate various state and federal statutes relating to privacy protections are each an independent and egregious breach of social norms.

178. The California Constitution created an inalienable right to be free from pervasive electronic surveillance; Plaintiff and Class Members are under no obligation to "opt out" of such violations of their constitutional privacy rights to stop Adobe's intrusions into their daily lives—that right inheres automatically for every Class Member.

179. The right to privacy in California's constitution creates a right of action for California residents against private entities such as Adobe. Adobe lacks a legitimate business interest in stockpiling and compiling the personal information of Plaintiff and Class Members.

180. Plaintiff and Class Members have been damaged by Adobe's invasion of their privacy and are entitled to just compensation and injunctive relief.

FOURTH CAUSE OF ACTION
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2510, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class)

181. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

182. The Federal Wiretap Act ("FWA"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.

183. In relevant part, the ECPA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring "any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

184. The ECPA protects both sending and receipt of communications.

185. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

186. The transmissions of Plaintiff's Private Information via Adobe's Tracking Tools qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

187. **Electronic Communications**. The transmission of Private Information between Plaintiff and Class Members and Adobe via its tracking technologies are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

188. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

189. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

190. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

(a) Cookie trackers

(b) Any other tracking code or SDK used by Adobe; and

(c) Segment Match.

191. Plaintiff and Class Members' interactions with each website are electronic communications under the ECPA.

192. By utilizing the tracking technologies, as described herein, Adobe intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class members in violation of 18 U.S.C. § 2511(1)(a).

193. Adobe intercepted communications that include, but are not limited to, communications to/from Plaintiff and Class Members regarding their health, travel, shopping habits, consumption of media, loan applications, and many more. This confidential information is then added to consumer profiles and monetized for targeted advertising purposes, among other things.

194. By intentionally using, or endeavoring to use, the contents of Plaintiffs' and Class Members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Adobe violated 18 U.S.C. § 2511(1)(d).

195. Adobe intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy, intrusion upon seclusion, CIPA, and other state wiretapping and data privacy laws, among others.

196. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, "[t]he association of Plaintiffs' data with preexisting user profiles is a further use of Plaintiffs' data that satisfies [the crime-tort] exception," because it "violate[s] state law, including the [CIPA], intrusion upon seclusion, and invasion of privacy." *Brown v. Google, LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021); *see also Marden v.LMND Medical Group, Inc.*, 2024 WL 4448684, at *2 (N.D. Cal. July 3, 2024); *R.C. v. Walgreen Co.*, 733 F. Supp. 3d 876, 902 (C.D. Cal. 2024).

197. Adobe was not acting under the color of law to intercept Plaintiff's and Class members' wire or electronic communications.

198. Plaintiff and Class Members did not authorize Adobe to acquire the content of their communications for purposes of invading Plaintiff's and Class Members' privacy. Plaintiff and Class members had a reasonable expectation that Adobe would not intercept their communications and sell their data to dozens of parties without their knowledge or consent.

199. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq*.

200. As a result of each and every violation thereof, on behalf of herself and the Class, Plaintiff seeks statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510, et seq. under 18 U.S.C. § 2520.

FIFTH CAUSE OF ACTION
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Nationwide Class)

201. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

202. To state a claim for intrusion upon seclusion "[Plaintiffs] must possess a legally protected privacy interest … [Plaintiffs'] expectations of privacy must be reasonable … [and Plaintiffs] must show that the intrusion is so serious in 'nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.'" *Hernandez v. Hillsides, Inc*. 47 Cal. 4th 272, 286-87 (2009).

203. Plaintiff and Class Members have an interest in: (i) precluding the dissemination and/or misuse of their sensitive, confidential communications and information; and (ii) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to highly intrusive surveillance at every turn.

204. By conducting such widespread surveillance, Adobe intentionally invaded Plaintiff's and Class Members' privacy rights, as well as intruded upon Plaintiff's and Class Members' seclusion.

205. Plaintiff's and Class Members had a reasonable expectation that their communications, identities, personal activities, health, and other data would remain confidential.

206. Plaintiff's and Class Members did not and could not authorize Adobe to intercept data on every aspect of their lives and activities.

207. The conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

(a) Defendants engage in widespread data collection and interception of Plaintiff's and Class Members' internet and app activity, including their communications with websites and apps, thereby learning intimate details of their daily lives based on the massive amount of information collected about them.

(b) Adobe combines the information collected on websites and apps with offline information also gathered on individuals to create Segment Match.

(c) Adobe create comprehensive profiles based on this online and offline data, which violates Plaintiff's and Class Members' common law right to privacy and the control of their personal information.

(d) Adobe sells or disclose these profiles, which contain the data improperly collected about Plaintiff and Class Members, to an unknown number of advertisers for use in the real-time-bidding process, which likewise violates Plaintiff's and Class Members' common law right to privacy and the control of their personal information.

208. Adobe's amassment of electronic information reflecting all aspects of Plaintiff's and Class Members' lives into profiles for future or present use is in and of itself a violation of their right to privacy in light of the serious risk these profiles pose to their autonomy.

209. In addition, those profiles are and can be used to further invade Plaintiff's and Class Members' privacy by, for example. allowing third parties to learn intimate details of their lives

and target them for advertising, political, and other purposes, as described herein, thereby harming them by selling this data to advertisers and other data brokers without their consent.

210. Accordingly, Plaintiff's and Class Members seek all relief available for invasion of privacy claims under common law.

RELIEF REQUESTED

Plaintiff, on behalf of herself and the proposed Class, respectfully requests that the Court grant the following relief:

(a) Certification of this action as a class action and appointment of Plaintiff and Plaintiff's counsel to represent the Class;

(b) A declaratory judgement that Defendant violated: (1) the Electronic Communications Privacy Act; (2) the California Invasion of Privacy Act; (3) Plaintiff's and Class Members' privacy rights as provided at common law and pursuant to the California Constitution; and (4) Plaintiff's and Class Members' other rights under common law;

(c) An order enjoining Adobe from engaging in the unlawful practices and illegal acts described herein; and

(d) An order awarding Plaintiff and the Class: (1) actual or statutory damages; (2) punitive damages—as warranted—in an amount to be determined at trial; (3) prejudgment interest on all amounts awarded; (4) injunctive relief as the Court may deem proper; (5) reasonable attorneys' fees and expenses and costs of suit pursuant to Cal. Code of Civil Procedure § 1021.5 and/or other applicable law; (6) pre-judgment and post-judgment interest as provided by law; and (7) such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the proposed Class, demands a trial by jury for all the claims asserted in this Complaint so triable.

Date: April 3rd, 2025

Respectfully submitted,

/s/ John J. Nelson
John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Fax: (865) 522-0049
Email: jnelson@milberg.com

/s/ Daniel O. Herrera
Daniel O. Herrera (*pro hac vice* forthcoming)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com

Counsel for Plaintiff and the Putative Class